IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:

Vincent Piel

Serial No.: 10/761,920

Filed: January 20, 2004

Confirmation No. 4097

Group Art Unit: 2135

Examiner: Patel, Nirav B.

Docket No. 500110459-2

For: Component for a Computer

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop: Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Appeal Brief under 37 C.F.R. § 41.37 is submitted in support of the Notice of Appeal filed February 26, 2008, responding to the final Office Action mailed September 27, 2007.

It is not believed that extensions of time or fees are required to consider this Appeal Brief. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. §1.136(a), and any fees required therefor are hereby authorized to be charged to Deposit Account No. 08-2025.

I. Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. Related Appeals and Interferences

There are no known related appeals or interferences that will affect or be affected by a decision in this Appeal.

III. Status of Claims

Claims 1-17 stand finally rejected. No claims have been allowed. The rejections of claims 1-17 are appealed.

IV. Status of Amendments

No amendments have been made subsequent to the final Office Action mailed September 27, 2007. The claims in the attached Claims Appendix (see below) reflect the present state of Applicant's claims.

V. Summary of Claimed Subject Matter

The claimed inventions are summarized below with reference numerals and references to the written description ("specification") and drawings. The subject matter described in the following appears in the original disclosure at least where indicated, and may further appear in other places within the original disclosure.

Embodiments according to independent claim 1 describe a component (Figure 3, 130) for a computer (Figure 1, 10). The component (Figure 3, 130) comprises a firmware element (Figure 1, 19) operable to perform a security check to verify the computer (Figure 1, 10) is connected to an authorized network (Figure 1, 17). The security check comprises generating a random number, Applicant's specification, page 3, lines 19-21, encrypting the random number with a public key of a public/private key pair associated with the network (Figure 1, 17), Applicant's specification, page 3, lines 21-22, and transmitting the encrypted random number to a network device (Figure 1, 18) via the network (Figure 1, 17). Applicant's specification, page 3, lines 22-24. The security check further comprises receiving a response comprising a number from the network device (Figure 1, 18) and permitting operation of at least a subsystem of the computer (Figure 1, 10) if the response is in accordance with the random number. Applicant's specification, page 3, lines 25-29. The step of permitting operation of at least a subsystem of the computer (Figure 1, 10) if the response is in accordance with the random number comprises comparing the random number transmitted to the network device (Figure 1, 18) with the number in the response and permitting operation if the number in the response matches the random number transmitted to the network device (Figure 1, 18), wherein the security check is performed when the computer (Figure 1, 10) is detected to have been in an unpowered state since a previous security check. Applicant's specification, page 3, lines 27-29 and page 4, lines 25-30.

Embodiments according to independent claim 10 describe a component (Figure 3, 130) for a computer (Figure 1, 10). The component (Figure 3, 130) comprises a firmware element (Figure 1, 19) operable to generate a random number to be used in performing a security check to verify the computer (Figure 1, 10) is connected to an authorized network (Figure 1, 17). Applicant's specification, page 3, lines 19-21. The firmware element is further operable to encrypt the random number with a public key of a public/private key pair associated with an authorized network (Figure 1, 17), Applicant's specification, page 3, lines 21-22, and transmit the encrypted random number to a network device (Figure 1, 18) via the network (Figure 1, 17). Applicant's specification, page 3, lines 22-24. Such a firmware element is also configured to receive a response comprising a number from the network device, Applicant's specification, page 3, lines 25-29, compare the random number transmitted to the network device with the number in the response, Applicant's specification, page 3, lines 25-29, and permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device, Applicant's specification, page 3, lines 25-29, wherein the security check is performed when the computer is detected to have been in an unpowered state since a previous security check. Applicant's specification, page 3, lines 27-29 and page 4, lines 25-30.

Embodiments according to independent claim 11 describe a BIOS (Figure 1, 12) for a computer (Figure 1, 10). The BIOS (Figure 1, 12) is operable to perform a security check to verify the computer (Figure 1, 10) is connected to an authorized network (Figure 1, 17) as part of a boot process. The security check comprises generating a random number, Applicant's specification, page 3, lines 19-21, encrypting the random number with a public key of a public/private key pair associated with the network (Figure 1, 17), Applicant's specification, page 3, lines 21-22, and transmitting the encrypted random number to a network device (Figure 1, 18) via the network (Figure 1, 17). Applicant's specification, page 3, lines 22-24. The security check further comprises receiving a response comprising a number from the network device (Figure 1, 18), Applicant's specification, page 3, lines 25-29, comparing the random number transmitted to the network device (Figure 1, 18) with the number in the response, Applicant's specification, page 3, lines 25-29, and preventing continuation of the boot process if the number in the response does not match the random number transmitted to the network device (Figure 1, 18), wherein the security check is performed in response to the computer (Figure 1, 10) being detected to have been in an unpowered state since a previous security check. Applicant's specification, page 4, lines 4-5 and page 4, lines 25-30.

Embodiments according to independent claim 12 describe a computer (Figure 1, 10) comprising a firmware element (Figure 3, 130) operable to perform a security check to verify the computer (Figure 1, 100) is connected to an authorized network (Figure 1, 17). The security check comprises generating a random number, Applicant's specification, page 3, lines 19-21, encrypting the random number with a public key of a public/private key pair associated with the network (Figure 1, 17), Applicant's specification, page 3, lines 21-22, and transmitting the encrypted random number to a network device (Figure 1, 18) via the network (Figure 1, 17). Applicant's specification, page 3, lines 22-24. The security check further comprises receiving a response comprising a number from the network device (Figure 1, 18), Applicant's specification, page 3, lines 25-29, and permitting operation of at least a subsystem of the computer (Figure 1, 10) if the response is in accordance with the random number. Applicant's specification, page 3, lines 25-29. The step of permitting operation of at least a subsystem of the computer (Figure 1, 10) if the response is in accordance with the random number comprises comparing the random number transmitted to the network device (Figure 1, 18) with the number in the response, Applicant's specification, page 3, lines 25-29, and permitting operation if the number in the response matches the random number transmitted to the network device (Figure 1, 18), Applicant's specification, page 3, lines 25-29, wherein the security check is performed in response to the computer (Figure 1, 10) being detected to have been in an unpowered state since a previous security check. Applicant's specification, page 3, lines 27-29 and page 4, lines 25-30.

Embodiments according to independent claim 17 describe a computer (Figure 1, 10) comprising an element (Figure 1, 12) operable to perform a security check to verify the computer (Figure 1, 10) is connected to an authorized network (Figure 1, 17) and a network device (Figure 1, 18) operable to receive a network enquiry from the computer (Figure 1, 10) over a network (Figure 1, 17). Applicant's specification, page 3, lines 22-24 and page 5, lines 24-28. The element (Figure 1, 12) is operable to generate a random number, Applicant's specification, page 3, lines 19-21, encrypt the random number with a public key of a public/private key pair associated with the network, Applicant's specification, page 3, lines 21-22, and transmit the encrypted random number to the network device (Figure 1, 18) via the network (Figure 1, 17). Applicant's specification, page 3, lines 22-24. The network device (Figure 1, 18) is operable to receive the encrypted random number from the computer (Figure 1, 10), Applicant's specification, page 3, lines 21-25, decrypt the encrypted random number using the private key of the public-private key pair, Applicant's specification, page 3, lines 24-25, and generate a response comprising the random number and transmit the response to the computer (Figure 1, 10). Applicant's specification, page 3, lines 25-27. The element (Figure 1, 12) is further operable to receive the response from the network device (Figure 1, 18), Applicant's specification, page 3, lines 25-29, compare the random number transmitted to the network device (Figure 1, 18) with the number in the response, Applicant's specification, page 3, lines 25-29, and permit operation of at least a subsystem of the computer (Figure 1, 10) if the number in the response matches the random number transmitted to the network device (Figure 1, 18), Applicant's specification, page 3, lines 25-29, wherein the security check is performed in response to the computer (Figure 1,

10) being detected to have been in an unpowered state since a previous security check. Applicant's specification, page 3, lines 27-29 and page 4, lines 25-30.

VI. Grounds of Rejection to be Reviewed on Appeal

The following grounds of rejections are to be reviewed on appeal:

Claims 1-17 have been rejected under 35 U.S.C. §103(a) as allegedly being anticipated by *Herzi* (U.S. Patent No. 6,484,262) in view of *Hamamoto* (U.S. Patent Publication No. 2002/0000913 A1).

VII. Arguments

The Appellant respectfully submits that Applicant's claims 1-17 are patentable under 35 U.S.C. §103. The Appellant respectfully requests that the Board of Patent Appeals overturn the final rejection of those claims at least for the reasons discussed below.

A. The *Herzi* Disclosure

Herzi describes that a security measure is implemented "upon every boot of the particular computer system," at regular intervals of time, or "any duration of time as may be established for a given security policy." *See* col. 4, lines 4-19. As such, *Herzi* fails to disclose that a security check is performed when the computer is detected to have been in an unpowered state since a previous security check.

B. The *Hamamoto* Disclosure

Hamamoto describes a monitoring device for an automatic teller machine, where a backup power supply is put in use for the monitoring device when the automatic teller machine is powered off. Accordingly, *Hamamoto* does not describe that a security check is performed when a computer is detected to have been in an unpowered state since a previous security check. Rather, *Hamamoto* describes that a backup power supply is used whenever the main power supply is unavailable.

C. Applicant's Claims 1-9

As provided in independent claim 1, Applicant claims:

> A component for a computer, the component comprising a firmware element operable to perform a security check to verify the computer is connected to an authorised network, the security check comprising the steps of:
>
> generating a random number,
>
> encrypting the random number with a public key of a public/private key pair associated with the network,
>
> transmitting the encrypted random number to a network device via the network,
>
> receiving a response comprising a number from the network device, and
>
> permitting operation of at least a subsystem of the computer if the response is in accordance with the random number,
>
> ***the step of permitting operation of at least a subsystem of the computer if the response is in accordance with the random number comprises comparing the random number transmitted to the network device with the number in the response and permitting operation if the number in the response matches the random number transmitted to the network device, wherein the security check is performed***

> ***when the computer is detected to have been in an unpowered state since a previous security check.***

(Emphasis added).

Applicant respectfully submits that independent claim 1 is allowable for at least the reason that *Herzi* in view of *Hamamoto* does not disclose, teach, or suggest at least "the step of permitting operation of at least a subsystem of the computer if the response is in accordance with the random number comprises comparing the random number transmitted to the network device with the number in the response and permitting operation if the number in the response matches the random number transmitted to the network device, wherein the security check is performed when the computer is detected to have been in an unpowered state since a previous security check," as emphasized above.

For example, *Herzi* describes that a security measure is implemented "upon every boot of the particular computer system," at regular intervals of time, or "any duration of time as may be established for a given security policy." *See* col. 4, lines 4-19. As such, *Herzi* fails to disclose that a "security check is performed when the computer is detected to have been in an unpowered state since a previous security check," as recited in claim 1. Further, *Herzi* does not describe the security check of claim 1 in the manner claimed.

Further, *Hamamoto* describes a monitoring device for an automatic teller machine, where a backup power supply is put in use for the monitoring device when the automatic teller machine is powered off. Accordingly, *Hamamoto* does not describe that a security check is performed when a computer is detected to have been in an unpowered state since a previous security check. Rather, *Hamamoto* describes that a backup power supply is used whenever the main power supply is unavailable. Therefore, *Hamamoto* fails to cure the deficiencies of the *Herzi* reference.

As a result, *Hamamoto* individually or in combination with *Herzi* does not teach or suggest at least "the step of permitting operation of at least a subsystem of the computer if the response is in accordance with the random number comprises comparing the random number transmitted to the network device with the number in the response and permitting operation if the number in the response matches the random number transmitted to the network device, wherein the security check is performed when the computer is detected to have been in an unpowered state since a previous security check," as recited in claim 1.

In the Advisory Action mailed January 22, 2008, the Examiner states that "Herzi teaches the security measure is performed upon every boot of the computer system . . . . Hamamoto's invention relates to a monitoring device for security which is capable of continuing to monitor for security, even if the device is in a power-off state or even if the device is powered down." Page 2. Accordingly, Applicant respectfully submits that neither reference discloses the detection of a computer being in an unpowered state from a previous security check or "the step of permitting operation of at least a subsystem of the computer if the response is in accordance with the random number comprises comparing the random number transmitted to the network device with the number in the response and permitting operation if the number in the response matches the random number transmitted to the network device, wherein the security check is performed when the computer is detected to have been in an unpowered state since a previous security check," as recited in claim 1.

For at least these reasons, *Herzi* in view of *Hamamoto* fails to establish a *prima facie* case of obviousness with respect to claim 1, and the rejection of claim 1 should be overturned.

Dependent claims 2-9 (which depend from independent claim 1) are allowable as a matter of law for at least the reason that dependent claims 2-9 contain all the features of allowable independent claim 1. For at least this reason, the rejections of claims 2-9 should be overturned.

D. Applicant's Claim 10

As provided in independent claim 10, Applicant claims:

> A component for a computer, the component comprising a firmware element operable to:
>
> generate a random number to be used in performing a security check to verify the computer is connected to an authorised network,
>
> encrypt the random number with a public key of a public/private key pair associated with an authorised network,
>
> transmit the encrypted random number to a network device via the network,
>
> receive a response comprising a number from the network device,
>
> compare the random number transmitted to the network device with the number in the response, and
>
> ***permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device, wherein the security check is performed when the computer is detected to have been in an unpowered state since a previous security check.***

(Emphasis added).

Applicant respectfully submits that independent claim 10 is allowable for at least the reason that *Herzi* in view of *Hamamoto* does not disclose, teach, or suggest at least to "permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device, wherein the security check is performed when the computer is detected to have been in an unpowered state since a previous security check," as emphasized above.

For example, *Herzi* describes that a security measure is implemented "upon every boot of the particular computer system," at regular intervals of time, or "any duration of time as may be established for a given security policy." *See* col. 4, lines 4-19. As such, *Herzi* fails to disclose to "permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device, wherein the security check is performed when the computer is detected to have been in an unpowered state since a previous security check," as recited in claim 10. Further, *Herzi* does not describe the security check of claim 10 in the manner claimed.

Further, *Hamamoto* describes a monitoring device for an automatic teller machine, where a backup power supply is put in use for the monitoring device when the automatic teller machine is powered off. Accordingly, *Hamamoto* does not describe that a security check is performed when a computer is detected to have been in an unpowered state since a previous security check. Rather, *Hamamoto* describes that a backup power supply is used whenever the main power supply is unavailable. Therefore, *Hamamoto* fails to cure the deficiencies of the *Herzi* reference.

As a result, *Hamamoto* individually or in combination with *Herzi* does not teach or suggest at least to "permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device, wherein the security check is performed when the computer is detected to have been in an unpowered state since a previous security check," as recited in claim 10.

In the Advisory Action mailed January 22, 2008, the Examiner states that "Herzi teaches the security measure is performed upon every boot of the computer system . . . . Hamamoto's invention relates to a monitoring device for security which is capable of continuing to monitor for security, even if the device is in a power-off state or even if the device is powered down." Page 2. Accordingly, Applicant respectfully submits that neither reference discloses the detection of a computer being in an unpowered state from a previous security check or to "permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device, wherein the security check is performed when the computer is detected to have been in an unpowered state since a previous security check," as recited in claim 10.

For at least these reasons, *Herzi* in view of *Hamamoto* fails to establish a *prima facie* case of obviousness with respect to claim 10, and the rejection of claim 10 should be overturned.

E. Applicant's Claim 11

As provided in independent claim 11, Applicant claims:

> A BIOS for a computer, the BIOS being operable to perform a security check to verify the computer is connected to an authorised network as part of a boot process, the security check comprising the steps of:
>
> generating a random number,
>
> encrypting the random number with a public key of a public/private key pair associated with the network,
>
> transmitting the encrypted random number to a network device via the network,
>
> receiving a response comprising a number from the network device, and
>
> comparing the random number transmitted to the network device with the number in the response; and
>
> ***preventing continuation of the boot process if the number in the response does not match the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check.***

(Emphasis added).

Applicant respectfully submits that independent claim 11 is allowable for at least the reason that *Herzi* in view of *Hamamoto* does not disclose, teach, or suggest at least "preventing continuation of the boot process if the number in the response does not match the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check," as emphasized above.

For example, *Herzi* describes that a security measure is implemented "upon every boot of the particular computer system," at regular intervals of time, or "any duration of time as may be established for a given security policy." *See* col. 4, lines 4-19. As such, *Herzi* fails to disclose "preventing continuation of the boot process if the number in the response does not match the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check," as recited in claim 11. Further, *Herzi* does not describe the security check of claim 11 in the manner claimed.

Further, *Hamamoto* describes a monitoring device for an automatic teller machine, where a backup power supply is put in use for the monitoring device when the automatic teller machine is powered off. Accordingly, *Hamamoto* does not describe that a security check is performed when a computer is detected to have been in an unpowered state since a previous security check. Rather, *Hamamoto* describes that a backup power supply is used whenever the main power supply is unavailable. Therefore, *Hamamoto* fails to cure the deficiencies of the *Herzi* reference. As a result, *Hamamoto* individually or in combination with *Herzi* does not teach or suggest at least "preventing continuation of the boot process if the number in the response does not match the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check," as recited in claim 11.

In the Advisory Action mailed January 22, 2008, the Examiner states that "Herzi teaches the security measure is performed upon every boot of the computer system . . . . Hamamoto's invention relates to a monitoring device for security which is capable of continuing to monitor for security, even if the device is in a power-off state or even if the device is powered down." Page 2. Accordingly, Applicant respectfully submits that neither reference discloses the detection of a computer being in an unpowered state from a previous security check or "preventing continuation of the boot process if the number in the response does not match the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check," as recited in claim 11.

For at least these reasons, *Herzi* in view of *Hamamoto* fails to establish a *prima facie* case of obviousness with respect to claim 11, and the rejection of claim 11 should be overturned.

F. Applicant's Claims 12-16

As provided in independent claim 12, Applicant claims:

> A computer comprising a firmware element operable to perform a security check to verify the computer is connected to an authorised network, the security check comprising the steps of:
>
> generating a random number,
>
> encrypting the random number with a public key of a public/private key pair associated with the network,
>
> transmitting the encrypted random number to a network device via the network,
>
> receiving a response comprising a number from the network device, and
>
> permitting operation of at least a subsystem of the computer if the response is in accordance with the random number,
>
> ***the step of permitting operation of at least a subsystem of the computer if the response is in accordance with the random number comprises comparing the random number transmitted to the network device with the number in***

> ***the response and permitting operation if the number in the response matches the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check.***

(Emphasis added).

Applicant respectfully submits that independent claim 12 is allowable for at least the reason that *Herzi* in view of *Hamamoto* does not disclose, teach, or suggest at least "the step of permitting operation of at least a subsystem of the computer if the response is in accordance with the random number comprises comparing the random number transmitted to the network device with the number in the response and permitting operation if the number in the response matches the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check," as emphasized above.

For example, *Herzi* describes that a security measure is implemented "upon every boot of the particular computer system," at regular intervals of time, or "any duration of time as may be established for a given security policy." *See* col. 4, lines 4-19. As such, *Herzi* fails to disclose "the step of permitting operation of at least a subsystem of the computer if the response is in accordance with the random number comprises comparing the random number transmitted to the network device with the number in the response and permitting operation if the number in the response matches the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check," as recited in claim 12. Further, *Herzi* does not describe the security check of claim 12 in the manner claimed.

In addition, *Hamamoto* describes a monitoring device for an automatic teller machine, where a backup power supply is put in use for the monitoring device when the automatic teller machine is powered off. Accordingly, *Hamamoto* does not describe that a security check is performed when a computer is detected to have been in an unpowered state since a previous security check. Rather, *Hamamoto* describes that a backup power supply is used whenever the main power supply is unavailable. Therefore, *Hamamoto* fails to cure the deficiencies of the *Herzi* reference.

As a result, *Hamamoto* individually or in combination with *Herzi* does not teach or suggest at least "the step of permitting operation of at least a subsystem of the computer if the response is in accordance with the random number comprises comparing the random number transmitted to the network device with the number in the response and permitting operation if the number in the response matches the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check," as recited in claim 12.

In the Advisory Action mailed January 22, 2008, the Examiner states that "Herzi teaches the security measure is performed upon every boot of the computer system . . . . Hamamoto's invention relates to a monitoring device for security which is capable of continuing to monitor for security, even if the device is in a power-off state or even if the device is powered down." Page 2. Accordingly, Applicant respectfully submits that neither reference discloses the detection of a computer being in an unpowered state from a previous security check or "the step of permitting operation of at least a subsystem of the computer if the response is in accordance with the random number comprises comparing the random number transmitted to the network device with the number in the response and permitting operation if the number in the response matches the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check," as recited in claim 12.

For at least these reasons, *Herzi* in view of *Hamamoto* fails to establish a *prima facie* case of obviousness with respect to claim 12, and the rejection of claim 12 should be overturned.

Dependent claims 13-16 (which depend from independent claim 12) are allowable as a matter of law for at least the reason that dependent claims 13-16 contain all the features of allowable independent claim 12. For at least this reason, the rejections of claims 13-16 should be overturned.

G. Applicant's Claim 17

As provided in independent claim 17, Applicant claims:

> In combination, a computer comprising an element operable to perform a security check to verify the computer is connected to an authorised network and a network device operable to receive a network enquiry from the computer over a network, the element being operable to:
>
> generate a random number,
>
> encrypt the random number with a public key of a public/private key pair associated with the network, and
>
> transmit the encrypted random number to the network device via the network,
>
> the network device being operable to:
>
> receive the encrypted random number from the computer,
>
> decrypt the encrypted random number using the private key of the public-private key pair, and
>
> generate a response comprising the random number and transmit the response to the computer;
>
> the element being operable to:
>
> receive the response comprising from the network device,
>
> compare the random number transmitted to the network device with the number in the response, and
>
> ***permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check.***

(Emphasis added).

Applicant respectfully submits that independent claim 17 is allowable for at least the reason that *Herzi* in view of *Hamamoto* does not disclose, teach, or suggest at least to "permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check," as recited and emphasized above in claim 17.

For example, *Herzi* describes that a security measure is implemented "upon every boot of the particular computer system," at regular intervals of time, or "any duration of time as may be established for a given security policy." *See* col. 4, lines 4-19. As such, *Herzi* fails to disclose to "permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check," as recited in claim 17. Further, *Herzi* does not describe the security check of claim 17 in the manner claimed.

In addition, *Hamamoto* describes a monitoring device for an automatic teller machine, where a backup power supply is put in use for the monitoring device when the automatic teller machine is powered off. Accordingly, *Hamamoto* does not describe that a security check is performed when a computer is detected to have been in an unpowered state since a previous security check. Rather, *Hamamoto* describes that a backup power supply is used whenever the main power supply is unavailable. Therefore, *Hamamoto* fails to cure the deficiencies of the *Herzi* reference.

As a result, *Hamamoto* individually or in combination with *Herzi* does not teach or suggest at least to "permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check," as recited in claim 17.

In the Advisory Action mailed January 22, 2008, the Examiner states that "Herzi teaches the security measure is performed upon every boot of the computer system . . . . Hamamoto's invention relates to a monitoring device for security which is capable of continuing to monitor for security, even if the device is in a power-off state or even if the device is powered down." Page 2. Accordingly, Applicant respectfully submits that neither reference discloses the detection of a computer being in an unpowered state from a previous security check or to "permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check," as recited in claim 17.

For at least these reasons, *Herzi* in view of *Hamamoto* fails to establish a *prima facie* case of obviousness with respect to claim 17, and the rejection of claim 17 should be overturned.

VIII. Conclusion

In summary, it is Applicant's position that Applicant's claims are patentable over the applied cited art references and that the rejection of these claims should be withdrawn. Appellant therefore respectfully requests that the Board of Appeals overturn the Examiner's rejection and allow Applicant's pending claims.

Respectfully submitted,

By: ____________________
Charles W. Griggers
Registration No. 47,283

Claims Appendix under 37 C.F.R. § 41.37(c)(1)(viii)

The following are the claims that are involved in this Appeal.

1. A component for a computer, the component comprising a firmware element operable to perform a security check to verify the computer is connected to an authorised network, the security check comprising the steps of:

generating a random number,

encrypting the random number with a public key of a public/private key pair associated with the network,

transmitting the encrypted random number to a network device via the network,

receiving a response comprising a number from the network device, and

permitting operation of at least a subsystem of the computer if the response is in accordance with the random number,

the step of permitting operation of at least a subsystem of the computer if the response is in accordance with the random number comprises comparing the random number transmitted to the network device with the number in the response and permitting operation if the number in the response matches the random number transmitted to the network device, wherein the security check is performed when the computer is detected to have been in an unpowered state since a previous security check.

2. A component according to claim 1 wherein the firmware element comprises a BIOS.

3. A component according to claim 2 wherein the firmware element is operable to perform a security check as part of a boot process.

4. A component according to claim 2 wherein the firmware element is operable to prevent operation of the computer if a valid response is not received.

5. A component according to claim 2 wherein the BIOS comprises a boot block and wherein the firmware element is stored in the boot block.

6. A component according to claim 1 wherein the firmware element comprises a controller for a peripheral.

7. A component according to claim 6 wherein the firmware element is operable to perform a security check in response to a transition to an operating state.

8. A component according to claim 6 wherein the firmware element is operable to prevent operation of the peripheral if a valid response is not received.

9. A component according to claim 6 wherein a network enquiry to verify the computer is connected to the authorised network is transmitted to a BIOS of the computer for transmission to the network device.

10. A component for a computer, the component comprising a firmware element operable to:

generate a random number to be used in performing a security check to verify the computer is connected to an authorised network,

encrypt the random number with a public key of a public/private key pair associated with an authorised network,

transmit the encrypted random number to a network device via the network,

receive a response comprising a number from the network device,

compare the random number transmitted to the network device with the number in the response, and

permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device, wherein the security check is performed when the computer is detected to have been in an unpowered state since a previous security check.

11. A BIOS for a computer, the BIOS being operable to perform a security check to verify the computer is connected to an authorised network as part of a boot process, the security check comprising the steps of:

generating a random number,

encrypting the random number with a public key of a public/private key pair associated with the network,

transmitting the encrypted random number to a network device via the network,

receiving a response comprising a number from the network device, and

comparing the random number transmitted to the network device with the number in the response; and

preventing continuation of the boot process if the number in the response does not match the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check.

12. A computer comprising a firmware element operable to perform a security check to verify the computer is connected to an authorised network, the security check comprising the steps of:

generating a random number,

encrypting the random number with a public key of a public/private key pair associated with the network,

transmitting the encrypted random number to a network device via the network,

receiving a response comprising a number from the network device, and

permitting operation of at least a subsystem of the computer if the response is in accordance with the random number,

the step of permitting operation of at least a subsystem of the computer if the response is in accordance with the random number comprises comparing the random number transmitted to the network device with the number in the response and permitting operation if the number in the response matches the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check.

13. A computer according to claim 12 wherein the firmware comprises a BIOS.

14. A computer according to claim 13 wherein the firmware element is operable to perform a security check as part of a boot process.

15. A computer according to claim 13 wherein the firmware element is operable to prevent operation of the computer if a valid response is not received.

16. A computer according to claim 13 wherein the BIOS comprises a boot block and wherein the firmware element is stored in the boot block.

17. In combination, a computer comprising an element operable to perform a security check to verify the computer is connected to an authorised network and a network device operable to receive a network enquiry from the computer over a network, the element being operable to:

generate a random number,

encrypt the random number with a public key of a public/private key pair associated with the network, and

transmit the encrypted random number to the network device via the network,

the network device being operable to:

receive the encrypted random number from the computer,

decrypt the encrypted random number using the private key of the public-private key pair, and

generate a response comprising the random number and transmit the response to the computer;

the element being operable to:

receive the response comprising from the network device,

compare the random number transmitted to the network device with the number in the response, and

permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device, wherein the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check.

Evidence Appendix under 37 C.F.R. § 41.37(c)(1)(ix)

There is no extrinsic evidence to be considered in this Appeal. Therefore, no evidence is presented in this Appendix.

Related Proceedings Appendix under 37 C.F.R. § 41.37(c)(1)(x)

There are no related proceedings to be considered in this Appeal. Therefore, no such proceedings are identified in this Appendix.